IN THE CLAIMS:

1. (Currently Amended) A method ~~to allow at least one party to perform at least one permitted activity with respect to a device~~, comprising ~~the steps of~~:

embedding a role certificate in ~~said device~~ a device, wherein the role certificate identifies ~~said~~ at least one permitted activity that at least one party is allowed to perform with respect to the device, and wherein the role certificate is generated by a Certification Authority (CA);

embedding at least information regarding a public key in said device the public key corresponding to the private key used by the CA to sign the role certificate; and

running the device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the device by said at least one party if the role certificate is verified,

wherein the at least one party communicates with the device to perform the permitted activity, after the role certificate is embedded in said device.

2. (Original) A method as defined in claim 1, wherein the role certificate includes information regarding a control security level for said device so that the device only allows said at least one permitted activity to be a type of action which is within the security level of the device as defined by the role certificate.

3. (Original) A method as defined in claim 2, wherein the security level defined by the role certificate allows a type of software code to be downloaded, and/or installed, and/or run on said device by said at least one party.

4. (Original) A method as defined in claim 3, wherein the type of software code is from the group of types of software code consisting of test code, production code and special code.

5. (Original) A method as defined in claim 4, wherein the special code can be code linked to a specific at least one party.

6. (Original) A method as defined in claim 3, wherein the role certificate further contains information with regard to a specific party of said at least one party that can download, and/or install, and/or run said type of software code.

7. (Original) A method as defined in claim 1, wherein the role certificate further contains information with regard to a specific party of said at least one party that can activate the at least one permitted activity within the device.

8. (Original) A method as defined in claim 7, wherein said information with regard to a specific party is a hash of information identifying said specific party's public key, and wherein the device validates said specific party by receiving said information identifying said specific party's public key, and hashing this information and comparing the hash value to the hash value contained in the role certificate so that if the hash values are equal, then the specific party is permitted to activate the at least one permitted activity.

9. (Original) A method as defined in claim 7, wherein said specific party is a group of entities.

10. (Original) A method as defined in claim 1, wherein the embedding of the role certificate into the device is performed after the information regarding the public key of the CA is embedded into the device.

11. (Original) A method as defined in claim 1, wherein the information regarding the CA public key is embedded in the device in a tamper resistant area.

12. (Original) A method as defined in claim 11, wherein the tamper resistant area of the device is a portion memory in the device such that any modification of information stored therein can be ascertained.

13. (Original) A method as defined in claim 1, wherein the role certificate contains information which causes said device to control the debugging facilities of said device with respect to said at least one party.

14. (Original) A method as defined in claim 1, wherein the CA is a root CA.

15. (Original) A method as defined in claim 1, wherein the device is a wireless device.

16. (Original) A method as defined in claim 1, wherein the CA is any entity other than said at least one party.

17. (Original) A method as defined in claim 1, wherein the role certificate may contain any use limitation with respect to said at least one permitted activity.

18. (Original) A method as defined in claim 17, wherein said any use limitation includes a time limitation with respect to activating said at least one permitted activity.

19. (Original) A method as deemed in claim 1, wherein said information regarding the CA public key is a hash value of said CA public key.

20. (Currently Amended) A role certificate mechanism ~~to permit at least one activity to be activated in a device~~, comprising:

memory within ~~the device~~ containing a role certificate, wherein the role certificate is configured to identify ~~identifies said~~ at least one activity permitted to be activated within a device in response to a communication, and further ~~where~~ wherein the memory contains information regarding a first key corresponding to a second key used to sign the role certificate; and

~~means~~ processor ~~for running~~ configured to run the device so as to verify the role certificate using said information regarding the first key so that said at least one permitted activity can be activated within the device,

wherein the role certificate mechanism is configured to receive the communication after the role certificate is embedded in said mechanism.

21. (Original) A role certificate mechanism as defined in claim 20, wherein the memory has a tamper resistant area and wherein said information regarding the first key is stored in said tamper resistant area.

22. (Original) A role certificate mechanism as defined in claim 20, wherein the role certificate further includes information regarding the identity of a third party, and wherein the means for verifying the role certificate includes means for reading said third party identity; wherein the role certificate mechanism further comprises means for receiving information from a third party and comparing at least a portion of said received information with the read third party identity from said role certificate, and if the comparison is the same, allowing said third party to perform said at least one activity on said device.

23. (Original) A role certificate mechanism as defined in claim 22, wherein said device is a mobile phone.

24. (Original) A role certificate mechanism as defined in claim 20, wherein said device is a mobile phone.

25. (Original) A role certificate mechanism as defined in claim 20, wherein said information regarding the first key is a hash of said first key.

26. (Currently Amended) An apparatus ~~to allow at least one party to perform at least one permitted activity with respect to a device~~, comprising:

means for embedding a role certificate in ~~said device~~ a device, wherein the role certificate identifies ~~said~~ at least one permitted activity that is allowed to be performed by at least one party with respect to the device, and wherein the role certificate is generated by a Certification Authority (CA);

means for embedding information regarding a public key in said device, the public key corresponding to the private key used by the CA to sign the role certificate; and

means for running the device so as to verify the role certificate using said information regarding the CA public key so that said at least one permitted activity can be activated within the device by said at least one party,

<u>wherein the at least one party communicates with the device to perform the permitted activity, only after the role certificate is embedded in said device</u>.

27. (Original) An apparatus as defined in claim 26, wherein the role certificate includes information regarding a control security level for said device so that the means for running the device provides that the at least one permitted activity to only be a type of action which is within the security level of the device as defined by the role certificate.

28. CANCEL

29. CANCEL.

30. CANCEL.

31. CANCEL.

32. CANCEL.

33. CANCEL.

34. CANCEL.

35. (Original) An apparatus as defined in claim 26, wherein the information regarding the CA public key is embedded in the device in a tamper resistant area.

36. (Original) An apparatus as defined in claim 26, wherein said information regarding the CA public key is a hash of said CA public key.

37. (Original) An apparatus as defined in claim 26, wherein the role certificate contains information which causes said device to control the debugging facilities of said device with respect to said at least one party.

38. (Original) An apparatus as defined in claim 26, wherein the device is a wireless device.

39. (Original) An apparatus as defined in claim 26, wherein the role certificate may contain any use limitation with respect to said at least one permitted activity.

40. (Original) An apparatus as defined in claim 39, wherein said any use limitation includes a time limitation with respect to activating said at least one permitted activity.

41. (Currently Amended) A method ~~to allow at least one party to perform at least one permitted activity that is applicable to a plurality of devices~~, comprising ~~the steps of~~:

embedding a role certificate applicable to ~~the plurality~~ a plurality of devices in an individual device, wherein the role certificate specifies ~~said~~ at least one permitted activity that is allowed to be performed by at least one party as applied to the plurality of devices, and wherein the role certificate is generated by a Certification Authority (CA);

embedding at least information regarding a public key applicable to the plurality of devices in said individual device, the public key corresponding to the private key used by the CA to sign the role certificate; and

running the individual device so as to verify the role certificate using said information regarding the CA public key so

that said at least one permitted activity can be activated within the individual device by said at least one party if the role certificate is verified,

wherein the at least one party communicates to perform the permitted activity, after the role certificate is embedded in said individual device.

42. (Previously Presented) The method of claim 41, wherein said individual device is also embedded with at least one different role certificate.

43. (Previously Presented) The method of claim 42, wherein one of the at least one different role certificate specifies at least a third party or a group or a device, and wherein the at least one permitted activity is not conducted if the one of the at least one different role certificate does not match said at least a third party or a group or a device.

44. CANCEL

45. (Previously Presented) The method of claim 1, wherein the role certificate includes a name of the Certification Authority that issued the certificate, a serial number, and an expiration date.

46. (Previously Presented) The method of claim 1, wherein the at least one party performs the at least one permitted activity by establishing a wireless connection to the device, and wherein the role certificate also identifies the at least one party.

47. (New) The method of claim 1, wherein the role certificate is embedded in said device during manufacture.

48. (New) The mechanism of claim 20, wherein the role certificate is embedded in said mechanism during manufacture.

49. (New) Apparatus, comprising:

means for storing a role certificate, wherein the role certificate is configured to identify at least one activity permitted to be activated within a device in response to a communication, and further wherein the means for storing the role certificate contains information regarding a first key corresponding to a second key used to sign the role certificate; and

means for running the device so as to verify the role certificate using said information regarding the first key so that said at least one permitted activity can be activated within the device,

wherein the communication occurs after the role certificate is embedded in said mechanism.

50. (New) An apparatus as defined in claim 49, wherein the means for storing the role cerificate has a tamper resistant area and wherein said information regarding the first key is stored in said tamper resistant area.